

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

---

In re Application of:	Jong-Uk CHOI et al.	Confirmation No.:	2206
Application No.:	10/034,485	Examiner:	Bayat, B.
Filed:	December 28, 2001	Group Art Unit:	3621
Customer No.:	30671		
Attorney Docket No.:	01122_1000		
Client Docket No.:	200601-0001/US		

---

For: METHOD FOR SECURING DIGITAL INFORMATION AND SYSTEM  
THEREFOR

**REPLY BRIEF UNDER 37 CFR §41.41**

Honorable Commissioner for Patents  
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is submitted in response to the Examiner's Answer dated February 26, 2008.

**I. RELATED APPEALS AND INTERFERENCES**

Under the heading of "Related Appeals and Interferences" on page 2 of the Examiner's Answer, the Examiner noted that, after the filing of the Appeal Brief, Appellants brought to the attention of the Honorable Board the filing of an Appeal Brief in U.S. Patent App. Serial No. 10/136,584, which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal. However, the Examiner's Answer did not also

include a listing of another such appeal, which was indicated in the Appeal Brief of the present application filed on November 27, 2007.

Accordingly, Appellants submit that the heading of “Related Appeals and Interferences” on page 2 of the Examiner’s Answer should also indicate the filing of an Appeal Brief on July 12, 2007, in U.S. Patent App. Serial No. 10/375,181, entitled “System For Protecting and Managing Digital Contents,” which may be related to, directly affect or be directly affected by or have a bearing on the Board’s decision in the present appeal.

## **II. MERITS OF “RESPONSE TO ARGUMENT” SECTION**

Pages 5-6 of the Examiner’s Answer set forth three paragraphs in response to the arguments presented by Appellants in the Appeal Brief. In the first and second paragraphs of the response, the Examiner appears to be citing the discussion of the conditional access agent 28<sup>1</sup> in paragraphs [0202], [0221], and [0222] of *Fransdonk* for the teaching of the features in claim 24 of the present application that were indicated in the Appeal Brief as not being disclosed in *Fransdonk*. In addition, the Examiner attempts to draw a comparison between these paragraphs in *Fransdonk* and the recitation in dependent claim 39, in order to bolster the Examiner’s analysis and conclusions. Appellants respectfully disagree with the assertions made and conclusions reached by the Examiner in the Examiner’s Answer.

---

<sup>1</sup> The first paragraph on page 5 of the Examiner’s Answer refers to “conditional access agent 48....” However, the reference numeral used in this instance appears to be in error, and the Appellants submit that the first paragraph should have read “conditional access agent 28....” This error is evident from a review of page 6 of the Appeal Brief and paragraph [0202] of *Fransdonk*, which are both referred to by the examiner when introducing the “conditional access agent” and both of which provide support for the assertion that the examiner is in fact referring to the conditional access agent 28. For example, *Fransdonk* uses reference numeral “28” for the “conditional access agent” and reference numeral “48” for the “conditional access client.” Additionally, *Fransdonk* refers to the conditional access agent 28 as generating a unique user key, and does not refer to the conditional access client as generating such a key.

The Examiner's Answer indicates that Appellants argued in the Appeal Brief that *Fransdonk* fails to disclose "creating a unique user key using system information of a user terminal" and that "the unique user key is transmitted by a user application tool installed in the user terminal for authentication," as recited in claim 24. In response, the Examiner's Answer cites paragraphs [0202], [0221], and [0222] of *Fransdonk*. However, Appellants assert that the analysis performed by the Examiner fails to fully and properly analyze several issues related to the above quoted portions of claim 24, and thus fail to establish anticipation. Thus, the Appellants maintain the position that the claims of the present application are not anticipated by *Fransdonk*.

Appellants note that the above quoted portions of claim 24 raise a first issue that relates to how the unique user key is created, and a second issue that relates to how the key is transmitted. Appellants submit that the analysis set forth by the Examiner is still unclear regarding both of these issues. In addition, the Appellants submit that the analysis set forth by the Examiner is still unclear even with regard to the most basic issues, such as which features of *Fransdonk* are being cited for the teaching of "a unique user key" and "a user terminal," which are clearly important to conducting an analysis of the first issue and the second issue.

With respect to the first issue, claim 24 specifies that the unique user key is created "using system information of a user terminal." And, with respect to the second issue, claim 24 specifies that the unique user key is transmitted "by a user application tool installed in the user terminal." Both of these features tie the unique user key to the user terminal in the manner recited. Thus, an understanding of which features of *Fransdonk* are being cited for the teaching of "a unique user key" and "a user terminal" is important for analyzing the first and second issues, and determining whether *Fransdonk* provides a teaching of all of the limitations of claim 24.

The first paragraph of the “Response to Argument” section of the Examiner’s Answer indicates that the “conditional access agent” 28<sup>2</sup> generates a unique user key, and the unique user key is then encrypted with a public key of the secure device 46. In light of this information, the Examiner concludes that *Fransdonk* “generates a unique user key utilizing system information of a user terminal (public key of the secure device)....” Thus, the first paragraph of the “Response to Argument” section of the Examiner’s Answer appears to address the first issue that relates to how the unique user key is created. The second paragraph of the “Response to Argument” section of the Examiner’s Answer discusses the transfer of content and keys with respect to paragraphs [0221]-[0222] and FIG. 8B of *Fransdonk*. Thus, the second paragraph of the “Response to Argument” section of the Examiner’s Answer appears to address the second issue that relates to how the unique user key is transmitted.

However, it is unclear from the Examiner’s Answer whether the Examiner is citing the unique user key ( $U_k$ ) discussed in *Fransdonk* for the teaching of the “unique user key” of claim 24, or whether the Examiner is citing the public key, or whether the Examiner is citing the encrypted unique user key ( $U_k$ ) (i.e., the unique user key ( $U_k$ ) encrypt using the public key), or whether the Examiner is citing some other key. Additionally, it is unclear from the Examiner’s Answer whether the Examiner is citing the conditional access agent 28 discussed in *Fransdonk* for the teaching of the user terminal, or whether the Examiner is citing the secure device 46, or whether the Examiner is citing some other device.

With respect to the first issue, claim 24 specifies that the unique user key is created “using system information of a user terminal.” In the first paragraph of the Examiner’s Answer, the Examiner appears to be asserting that the “unique user key” is the encrypted version of the unique

---

<sup>2</sup> As noted above, the conditional access agent in *Fransdonk* is given reference numeral 28.

user key ( $U_k$ ), which is encrypted using the public key of the secure device 46. Appellants assert, however, that *Fransdonk* does not disclose that the public key of the secure device 46 is **created using system information** of a user terminal, regardless of whether the secure device 46 or the conditional access agent 28 is considered to be the user terminal. The public key is described as being “of the secure device 46;” however, such a statement does not indicate that it is created **using system information** of the secure device 46 (or of the conditional access agent, for that matter). Additionally, no other evidence is presented by the Examiner for such a teaching. Also, the use of such a public key to encrypt another key does not by itself render the resulting encrypted key as being created using system information, and *Fransdonk* does not provide such a teaching.

If, on the other hand, the first paragraph of the “Response to Argument” section of the Examiner’s Answer is asserting that the feature of *Fransdonk* being cited for the teaching of the “unique user key” of claim 24 is the unique user key ( $U_k$ ), then attention is drawn to the arguments set forth in the Appeal Brief regarding this issue. In summary, as noted in the Appeal Brief, *Fransdonk* does not specifically indicate that the “unique user key ( $U_k$ )” generated by the conditional access agent 28 is created **using system information of a user terminal**, but merely that it is created after the verification process. The fact that a key is a unique user key does not indicate that it was created using system information of a user terminal. *Fransdonk* does not specifically indicate that the “unique user key ( $U_k$ )” generated by the conditional access agent 28 is created using system information of conditional access agent 28. Furthermore, even if it is assumed solely for the sake of argument, that the unique user key ( $U_k$ ) is created using system information of the secure device 46 (which Appellants do not concede), the unique user key ( $U_k$ ) is not described as being transmitted by a user application tool installed in the secure device 46.

Additionally, with respect to the other keys mentioned in the second paragraph of the “Response to Argument” section of the Examiner’s Answer, such as the product keys, session keys, private keys, and secret keys, these keys are also not described in *Fransdonk* as being created **using system information of a user terminal**.

The second paragraph of the “Response to Argument” section of the Examiner’s Answer discusses the transfer of content and keys with respect to paragraphs [0221]-[0222] and FIG. 8B of *Fransdonk*. Thus, the second paragraph of the “Response to Argument” section of the Examiner’s Answer appears to address the second issue that relates to how the unique user key is transmitted. Claim 24 specifies that the unique user key is transmitted “by a user application tool installed in the user terminal.” Thus, the unique user key, which is created “using system information of a user terminal,” is further defined as being “transmitted by a user application tool installed in the user terminal....” Appellants assert, however, that *Fransdonk* does not disclose such a combination of features.

The second paragraph of the “Response to Argument” section of the Examiner’s Answer notes that the conditional access agent 28 encrypts the session keys with the unique user key ( $U_k$ ) and send the encrypted session keys to the conditional access client 48, as indicated at 108 in FIG. 8B, and distributes the unique user key ( $U_k$ ) to the conditional access client 48 via a secure authorization channel, as indicated at 110. As described in paragraph [0222] of *Fransdonk*, the unique user key ( $U_k$ ) is used to decrypt the session keys, which are then used to decrypt encrypted content 26 received via another channel. However, at no time during this procedure does *Fransdonk* describe a key, which is created using system information of a terminal, being transmitted by that terminal. The second paragraph of the “Response to Argument” section of the Examiner’s Answer appears to indicate that the unique user key ( $U_k$ ) is being cited as the unique

user key in claim 24; however, only the conditional access agent 28 is described as transmitting the unique user key ( $U_k$ ) and *Fransdonk* does not indicate that the unique user key ( $U_k$ ) is created using system information of conditional access agent 28.

In the third paragraph of the “Response to Argument” section of the Examiner’s Answer, the Examiner compares the procedures performed in paragraphs [0221]-[0222] of *Fransdonk* with the limitations recited in claim 39 for support for the conclusions set forth in the Examiner’s Answer. The Examiner refers to the “user authentication process” in claim 39 as merely a comparison of the unique user key as in paragraphs [0221]-[0222]. Appellants respectfully disagree.

In paragraphs [0221]-[0222] of *Fransdonk*, three items are sent to the conditional access client 48, namely, encrypted session keys (encrypted with the unique user key ( $U_k$ )) from the conditional access agent 28 via 108, the unique user key ( $U_k$ ) from the conditional access agent 28 via a secure authorization channel 110, and encrypted content 26 via another channel from the content provider 16. In paragraphs [0221]-[0222], *Fransdonk* does not mention the authentication of the unique user key ( $U_k$ ) by the conditional access client 48, but rather sends the unique user key ( $U_k$ ) via a secure authorization channel, which presumably the conditional access client 48 would trust without further authentication of data received once the secure authorization channel was established. The conditional access client 48 then merely uses the unique user key ( $U_k$ ) to decrypt the session keys.

Contrary to the description in paragraphs [0221]-[0222] of *Fransdonk*, the portion of claim 39 referred to by the Examiner recites “performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication.” Thus, in claim

39, a user authentication process is performed by comparing a stored key to a subsequently transmitted key. No such comparison is discussed in paragraphs [0221]-[0222] of *Fransdonk*. Paragraphs [0221]-[0222] of *Fransdonk* do not discuss authentication of the unique user key ( $U_k$ ), but merely discuss receipt of the unique user key ( $U_k$ ) and use of the unique user key ( $U_k$ ) to decrypt the encrypted session keys.

Thus, Appellants submit that the Examiner's attempted comparison between the "user authentication process" in claim 39 and the procedures discussed in paragraphs [0221]-[0222] of *Fransdonk* in fact highlights distinctions therebetween.

### **III. CONCLUSION AND PRAYER FOR RELIEF**

For the foregoing reasons, as well as for the reasons set forth in the Appeal Brief filed on November 27, 2007, Appellants maintain their position that claims 24-26 and 39 are not anticipated under 35 U.S.C. §102 by *Fransdonk*. Accordingly, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,  
DITTHAVONG MORI & STEINER, P.C.

April 28, 2008  
Date

/Christopher D. Ward/  
Christopher D. Ward  
Attorney for Appellant(s)  
Reg. No. 41367

918 Prince Street  
Alexandria, VA 22314  
Tel. 703-519-9952  
Fax. 703-519-9958